

Benefícios**Compacto e Conveniente**

O iKey 2032 é do tamanho de um pendrive, mas oferece a seu usuário recursos de segurança sem paralelo no mercado

Fácil de transportar

Devido ao seu tamanho pequeno e estrutura resistente, o iKey 2032 permite que os usuários sempre tenham suas identificações digitais exclusivas à mão

Conectividade USB**Fácil de Implantar**

O iKey 2032 oferece a segurança de um smart card sem a necessidade de uma leitora de smart card. Sua porta USB 1.1/2.0 pode conectá-lo a qualquer computador

Para aprimorar os aplicativos de segurança, não é necessário implantar e manter leitoras de smart card de custo elevado ou dispositivos biométricos especiais: o iKey oferece a segurança do smart card sem as suas dores de cabeça, como a da questão da interoperabilidade entre leitoras e padrões.

Processamento de Criptografia On-board

Ao contrário de outros sistemas de autenticação de smart card ou baseados em tokens, o iKey 2032 oferece criação de chaves e processamento de criptografia on-board para garantir que as funções e chaves criptografadas jamais fiquem desprotegidas

O primeiro token "verde" do mercado

O iKey 2032 também é aderente às normas internacionais de preservação do meio ambiente, e detém a certificação ROHS (Restriction on Hazardous Substances (RoHS, ou Restrição a Substâncias Perigosas), assegurando a seus usuários que o produto está livre de chumbo e cádmio.

SafeNet iKey

Seu dispositivo definitivo de autenticação pessoal para certificação digital



A linha SafeNet iKey®, que o mercado brasileiro conhece através do tradicional iKey 2032®, lança agora o iKey 4000®, o token de autenticação mais completo do mercado. Ele chega com certificação FIPS 140-2/Nível 2, ROHS (Restriction on Hazardous Substances*), China ROHS, FCC Part 15/Classe B, e CE), com suporte para qualquer aplicativo baseado — ou não — em certificação digital, e roda em qualquer ambiente operacional.

Token definitivo para autenticação

O iKey 2032 da SafeNet é um dispositivo USB de autenticação para certificação digital, que gera e armazena até 10 chaves privadas, incluindo a cadeia de certificados. Extensão da tecnologia de smart card, o iKey 2032 pode ser conectado a qualquer porta USB e fornece autenticação forte (dois fatores) de usuários sem a necessidade de leitoras de cartão. O iKey 2032 foi projetado para ser compatível com uma grande variedade de aplicativos para desktop e sistemas portáteis. Devido ao seu baixo custo, design compacto e interface USB padrão, é mais fácil de implantar e gerenciar do que os smart cards. Seu hardware tem certificação FIPS nível 2 e seus recursos incorporados de criação e armazenamento de chaves criptográficas, assinatura digital e robustez física fornecem segurança inigualável a qualquer software cliente.

Senhas fracas são eliminadas com a autenticação forte

O iKey 2032 fornece autenticação de dois fatores para aplicativos em que a segurança seja um fator crítico. Ao contrário da autenticação de senhas tradicional, que utiliza senhas fracas, que podem ser facilmente descobertas, o iKey 2032, para concluir o processo de autenticação, requer o token físico (o próprio iKey com a chave privada exclusiva do usuário) e o PIN do usuário.

Compatível com milhares de aplicativos de segurança

A SafeNet vem trabalhando com desenvolvedores de segurança para garantir que o iKey ofereça suporte a uma grande variedade de soluções. Hoje, pode-se usar o iKey em aplicações de logon, logon com smart card, single sign-on, autenticação em VPNs, criptografia de emails, assinaturas digitais, acesso a arquivos criptografados, e em muitos aplicativos de certificação dos principais fornecedores no Brasil, como Certisign, Serasa, Serpro, Microsoft, Computer Associates, VeriSign e outros. Inteiramente compatível com a ICP Brasil, o iKey 2032 também opera com PKCS#11 e MS Crypto API para integração com aplicativos mais personalizados.

Mais segurança, com a certificação FIPS 140-1 L2

O iKey 2032 está validado pelo padrão FIPS 140-1, nível 2 (certificado 161) com a finalidade de oferecer proteção superior aos aplicativos que requerem alto nível de segurança física, lógica e funcional. E não é apenas o chip onde se processam as operações: toda a sua carcaça foi certificada, o que a torna inviolável.

(*) Restrição a substâncias perigosas (como chumbo e cádmio)



Utilizado por vários aplicativos de segurança no mundo inteiro

O iKey 2032 foi integrado com vários aplicativos, inclusive no logon com smart card e single sign-on, autenticação em VPNs, criptografia de e-mails, assinaturas digitais e em muitos aplicativos para certificação digital dos principais fornecedores, como Certisign, Serasa, Serpro, Microsoft, Computer Associates, VeriSign e outros. O iKey 2032 é compatível com o PKCS#11 e a Microsoft CryptoAPI para uma melhor integração com aplicativos personalizados.

Compacto e conveniente

Embora o iKey 2032 seja do tamanho de um pendrive, ele oferece grandes recursos de segurança. Fácil de transportar, devido ao seu tamanho pequeno e estrutura resistente, possibilita que os usuários sempre tenham suas identidades digitais exclusivas à mão.



A SafeNet oferece uma suite completa de produtos que utilizam tecnologia criptográfica para a proteção de transações eletrônicas, dados em repouso e identidades digitais. As soluções da SafeNet são empregadas em todo o mundo por muitas empresas da Fortune 1000, mais de 1500 bancos, incluindo 13 dos 15 primeiros bancos americanos e agências de governo deste país tais como o Federal Reserve e o FBI. Presente no Brasil desde 2004, com sede em Alphaville, São Paulo, a empresa está presente através de 40 canais certificados em todo o país - todos especializados em segurança e com alto nível de qualificação técnica.

Com mais de 5.000 clientes em todo o mundo, a SafeNet está presente em 100 países, com escritórios próprios e canais de distribuição. Alguns de seus principais clientes são: Serpro, Banco Itaú, Caixa Econômica Federal, Certisign, Serasa, Imprensa Oficial do Estado de São Paulo, Bradesco, Microsoft, Bank of America, Citibank, Cisco Systems, Departamento de Defesa dos EUA, Deutsche Bank, Banco Ibi, Samsung, Texas Instruments, Receita Federal Americana, VIVO, Telefonica, Brasil Telecom, Embratel.

<http://br.safenet-inc.com>



SafeNet Brasil

Alameda Tocantins, 280
06455-020 - Barueri - São Paulo
TEL FAX: +55(11)4208-7700
<http://br.safenet-inc.com>

SafeNet Brasil© - Todos os direitos reservados. As informações constantes neste folheto podem ser alteradas sem aviso prévio. A SafeNet não assume responsabilidade por quaisquer erros que eventualmente possam ser identificados neste folheto.

Especificações Técnicas

Requisitos do Sistema

Sistemas Operacionais com Suporte:

- Microsoft Windows 95, Windows 98, Windows NT (SP4), Windows 2000, Windows XP, Vista e Linux

APIs de Criptografia

- PKCS#11 v 2.01
- Microsoft CryptoAPI (CAPI) 2.0
- Microsoft PC/SC

Validação de Hardware

de Criptografia

- Certificado no padrão FIPS 140-1 nível 2 - certificado nº 161

Funções de Criptografia

- Criação assimétrica de pares de chaves (RSA)
- Criação simétrica de chaves (DES, 3DES, RC2)
- Armazenamento e gerenciamento de chaves protegidos por hardware
- Assinatura digital incorporada
- Desempenho da Criptografia
- Operações de chaves RSA de 1024 e 2048 bits
- Criação de chaves: menos de 90 segundos com verificação da chave
- Assinatura digital: menos de 1 segundo

Algoritmos de Criptografia

Criptografia Assimétrica de Chaves

- RSA de 1024 bits, RSA de 2048 bits

Algoritmos Simétricos de Chaves

- DES, 3DES, RC2
- Assinatura Digital
- RSA de 1024 bits, RSA de 2048 bits
- Algoritmos de Hash
- SHA-1, MD5

Suporte a algoritmos adicionais disponível

Características Físicas

Hardware

- Processador de 8 bits
- Memória de 32 K

Conectividade

- Compatível com USB 1.1/2.0
- Transferência de 1,5 Mbits por segundo

Dimensões

- 15,875 mm x 57,15 mm x 7,9375 mm

Normas Reguladoras

- FCC Parte 15 - classe B CE

O iKey2032 pode ser produzido com logotipos personalizados. Consulte seu representante SafeNet.

